North Carolina Security Breach Reporting Form
Pursuant to the Identity Theft Protection Act of 2005

*Indicated a mandatory field

*Name of the Company or Government Agency owning or licensing information affected by the entity experiencing breach:

HEMENWAY & BARNES LLP AND HEMENWAY TRUST COMPANY

Entity Type:	GENERAL BUSINESS
Address:	75 STATE STREET
Apt/Suite/Building:	16TH FLOOR
City:	BOSTON
State:	MA
Zip Code:	02109
Telephone:	(617) 227-7940
Fax:	
Email:	

*Date Security breach Reporting Form Submitted:	11/02/2018
Is this notice a supplement to a previously filed Security Breach:	NO
*Date the Security Breach was discovered:	09/01/2018
Breach Type:	HACKERS/ UNAUTHORIZED ACCESS
*Estimated number of affected individuals:	2116
*Estimated number of NC residents affected:	16

Name of company or government agency maintaining or possessing information that was the subject of the Security Breach, if the agency that experienced the Security Breach is not the same entity as the agency reporting the Security Breach (pursuant to N.C.G.S. 75-65(b))

Describe the circumstances surrounding the Security Breach:

HEMENWAY & BARNES AND HEMENWAY TRUST COMPANY ("HEMENWAY") IS A LAW FIRM BASED IN MASSACHUSETTS. ON SEPTEMBER 1, 2018, HEMENWAY DISCOVERED THAT AN UNAUTHORIZED PERSON GAINED ACCESS TO SOME OF ITS EMPLOYEES' EMAIL. WHEN HEMENWAY LEARNED ABOUT THE UNAUTHORIZED ACCESS, IT IMMEDIATELY SECURED THE EMAIL ACCOUNTS, BEGAN AN INVESTIGATION AND ENGAGED A LEADING FORENSIC FIRM. HEMENWAY CONDUCTED A THOROUGH REVIEW OF THE EMAIL ACCOUNTS AND DETERMINED ON OCTOBER 24, 2018 THAT AN EMAIL OR EMAIL ATTACHMENT IN ONE OF THE ACCOUNTS CONTAINED PERSONAL INFORMATION THAT INCLUDED THE NAME AND SOCIAL SECURITY NUMBER OR CHECKING ACCOUNT NUMBER OF 16 NORTH CAROLINA RESIDENTS.

BEGINNING TODAY, NOVEMBER 2, 2018, HEMENWAY IS MAILING A NOTIFICATION LETTER BY U.S. MAIL TO THE POTENTIALLY AFFECTED NORTH CAROLINA RESIDENTS. HEMENWAY IS AVAILABLE TO SPEAK WITH POTENTIALLY AFFECTED INDIVIDUALS AND HAS OFFERED ONE YEAR OF FREE CREDIT MONITORING SERVICES TO POTENTIALLY AFFECTED INDIVIDUALS.

TO HELP PREVENT SOMETHING LIKE THIS FROM HAPPENING IN THE FUTURE, HEMENWAY CONTINUES TO ENHANCE ITS CYBERSECURITY DEFENSES AND PROCEDURES TO DETECT IMPROPER ACCESS TO ITS SYSTEMS.

THIS REPORT DOES NOT WAIVE HEMENWAY'S OBJECTION THAT NORTH CAROLINA LACKS PERSONAL JURISDICTION REGARDING THE COMPANY RELATED TO THIS MATTER.

Information Type:	ACCOUNT # SSN
*Regarding information breached, if electronic, was the information protected in some manner:	YES
If YES, please describe the security measures protecting the information:	INFORMATION WAS CONTAINED IN PASSWORD PROTECTED EMAIL ACCOUNTS.
*Describe any measures taken to prevent a similar Security Breach from occurring in the future:	TO HELP PREVENT SOMETHING LIKE THIS FROM HAPPENING IN THE FUTURE, HEMENWAY CONTINUES TO ENHANCE ITS CYBERSECURITY DEFENSES AND PROCEDURES TO DETECT IMPROPER ACCESS TO ITS SYSTEMS.
*Date affected NC residents were/will be notified:	11/02/2018
Describe the circumstances surrounding the delay in notifying affected NC residents pursuant to N.C.G.S. 75-65 (a) and (c):	THERE WAS NO DELAY IN NOTIFYING NORTH CAROLINA RESIDENTS. HEMENWAY DETERMINED NC RESIDENTS WERE AFFECTED ON 10/24/2018.

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. 75-65(c), please attach or mail the written request or the contemporaneous memorandum.

How NC residents were/will be notified? (pursuant to N.C.G.S. 75-65 (e)): WRITTEN NOTICE

Please note if the business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000) or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information or consent to satisfy subdivisions (1), (2) , or (3) of this subsection, for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following:

- Email notice when the business has an electronic mail address for the subject persons
- Conspicuous posting of the notice on the Web site page of the business, if one is maintained
- Notification to major statewide media

Please attach a copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

Contact Information Affiliation with entity experiencing breach: ATTORNEY

Organization Name: BAKER & HOSTETLER LLP

Prefix: MR

*First Name: RANDAL

Middle Name:

*Last Name: GAINER

Suffix:

Title: PARTNER

Address: 999 THIRD AVENUE

Apt/Suite/building: SUITE 3600

City: SEATTLE

State: WA Zip Code: 98104

*Telephone: (206) 332-1381 Fax:

Email: RGAINER@BAKERLAW.COM

C/O Epiq
PO Box 10662
Dublin, OH 43017-9252

<<Name 1>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

November 2, 2018

Dear <<Name1>>:

We at Hemenway & Barnes LLP and Hemenway Trust Company strive to offer you the highest level of service and attention and understand the importance of protecting your personal information. We take many precautions with our use of technology and have implemented operational procedures designed to protect your personal information. Unfortunately, we are writing to inform you that we recently identified and addressed an incident that involved some of your personal information. This letter describes the incident, measures we have taken and some steps you can take in response. We are available and committed to assisting you with the steps described below.

On September 1, 2018, we determined that an unauthorized person had accessed some of our employees' email accounts. We immediately secured the accounts, began an investigation and engaged a leading computer forensic firm to assist us. Through the investigation, we determined that the unauthorized person accessed a number of emails in the accounts. We conducted a thorough review of the impacted email accounts and determined on October 24, 2018 that an email or email attachment in one of the accounts contained some of your personal information, including your name or account name, or both, your Social Security number<variable data>.

Although we have no evidence that your personal information has been misused in any way, we are offering you a one-year membership in Experian's® IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on IdentityWorks Credit 3B, including instructions on how to activate your one-year membership, as well as some additional steps you can take in response to the incident described above, please see the information provided with this letter. We are also available to help with setting up this monitoring service.

We regret this incident occurred and apologize for the inconvenience and concern it may cause. We take seriously our obligation to do all that we can to protect you and your personal information, and we continue to enhance our cybersecurity defenses and procedures to detect improper access to our systems. If you have questions about the incident or the information that was accessed, or if you would like help in setting up your monitoring, please call your H&B or HTC advisor at (617) 227-7940.

Sincerely,

HEMENWAY & BARNES, LLP

Kurt F. Somerville, Managing Partner

HEMENWAY TRUST COMPANY LLC

Stephen W. Kidder, President

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by **February 3, 2019** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code**: **[Code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

More Information Regarding Ways to Protect Yourself

Regardless of whether you take advantage of the free credit monitoring, we recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you detect any unauthorized activity on your financial accounts, you should immediately contact your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center**,** 600 Pennsylvania Avenue NW
Washington, DC 20580, www.ftc.gov/idtheft, 1-877-IDTHEFT (438-4338),

If you are a resident of Connecticut, Maryland, or **North Carolina**, you may contact and obtain information from your state attorney general at:

Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106
www.ct.gov/ag, 1-860-808-5318

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202
www.oag.state.md.us, 1-888-743-0023 (toll free when calling within Maryland)
1-410-576-6300 (for calls originating outside Maryland)

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov,
1-919-716-6400 or toll free at 1-877-566-7226

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. There is no fee to place or lift a credit freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

To place a security freeze on your credit report, you must submit a request through a toll-free telephone number, a secure electronic system maintained by the credit reporting agency, or by sending a written request via regular, certified, or overnight mail. To place a security freeze on your credit report, contact each of the credit reporting agencies at the addresses below:

Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com
Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic system maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic system maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit.

The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Experian, TransUnion and Equifax – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. And you must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.